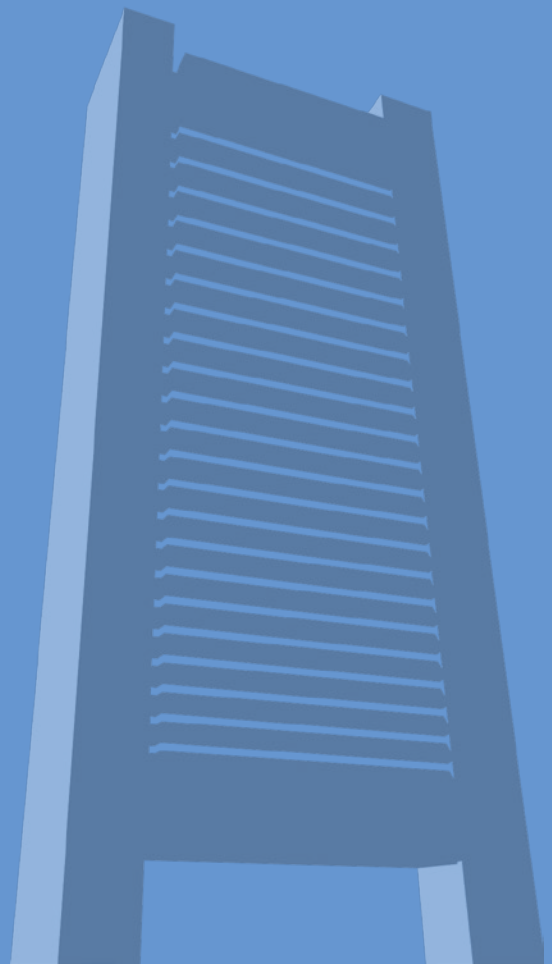
FEDERAL RESERVE BANK OF BOSTON™

EMBARGOED UNTIL FRIDAY, JANUARY 30, 2015 AT 2:45 A.M. IN U.S. EASTERN TIME AND 9:45 A.M. IN CAPE TOWN, SOUTH AFRICA; OR UPON DELIVERY



Cyber Security and Financial Stability

Eric S. Rosengren
President & CEO
Federal Reserve Bank of Boston

January 30, 2015

BCBS-FSI High-level Meeting for Africa on “Strengthening Financial Sector Supervision and Current Regulatory Priorities”
Cape Town, South Africa

bostonfed.org

Central Banks and Payments

- Safety, security, and efficiency of payment systems is an important role for central banks
- Payment system innovation has generated a less bank-centric system that is evolving faster than the regulatory framework
- I will discuss today why financial stability and cyber security of payments are so closely linked

Impact of Innovations in Payments

- Lower costs and more flexible payments options for consumers and businesses
- However, cyber-security issues are beginning to intrude on the benefits of some of these innovations
- From the inconvenience of denial of transaction to more serious identity theft, households are being affected
- Firms are also impacted by collateral problems with electronic payments – resulting in a wide variety of proprietary information being misappropriated

Financially Motivated Cyber Threats

- Traditional purpose of attack – financial gain
- Strategies to contain attacks focused on financial gain:
  - First, prevent the intruder from entering the system
  - Second, and often more importantly, prevent the intruder's ability to leave the system with confidential data
  - Third, devalue the data so it is meaningless to an intruder

Rogue States and Cyber Security

- Different purpose of attack – causing disruption of payments and economic activity is the goal
- These attacks have become much more disruptive
  - Initially, used brute-force “denial of service”
  - Penetrating and disrupting payments and records is now a greater risk
- This highlights the need for defense-grade security level, not just commercial-grade security level

U.S. Payments Systems

- Federal Reserve Banks process over $4 trillion in transactions per day
- Wholesale payments – for example, Fedwire Funds transfers, Fedwire Securities transactions, and CHIPS
- Retail payments – Automated Clearinghouse (ACH) payments, credit card payments, debit card payments, PayPal, Google Wallet or Apple Pay

Figure 1: Retail Authorization

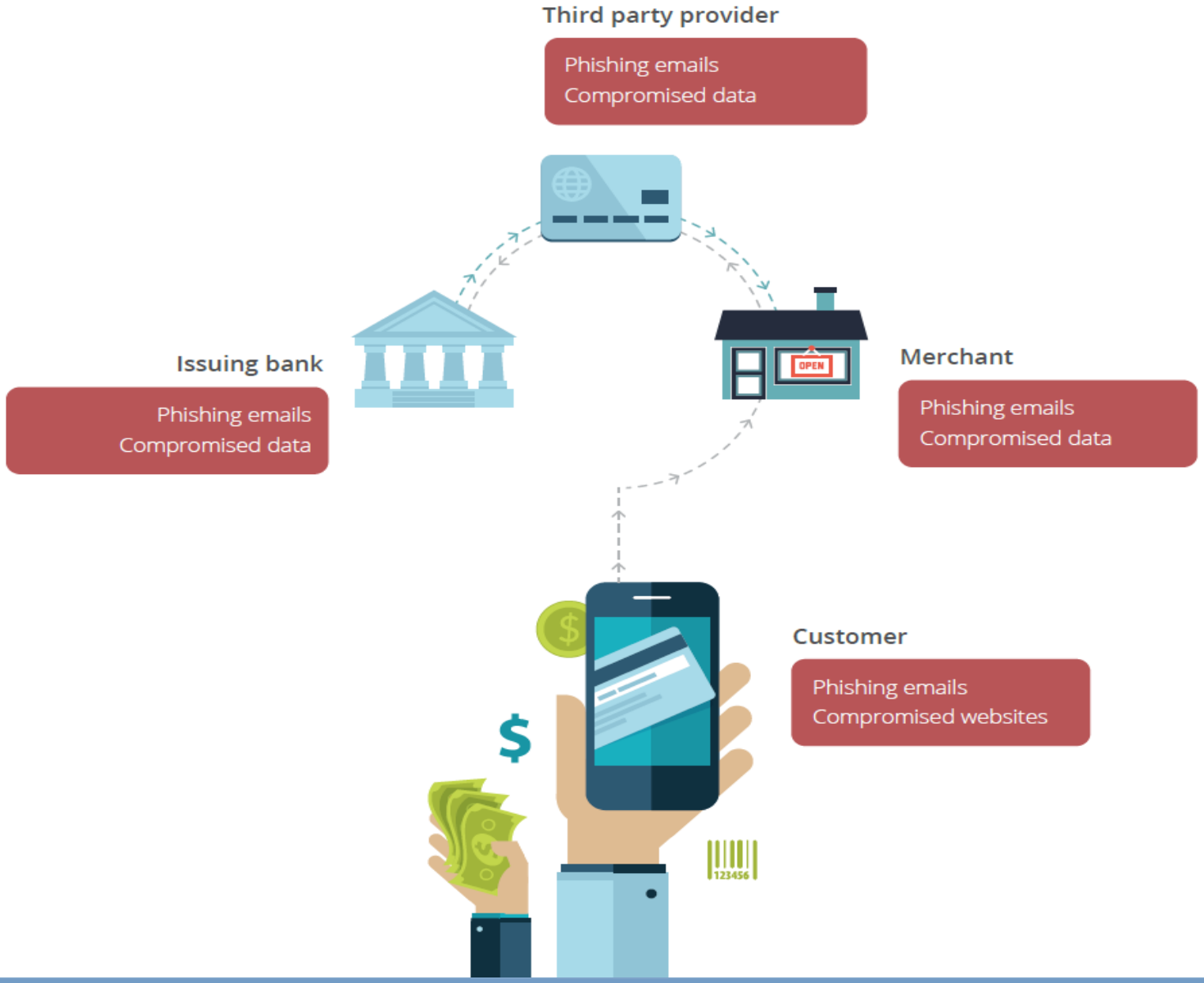
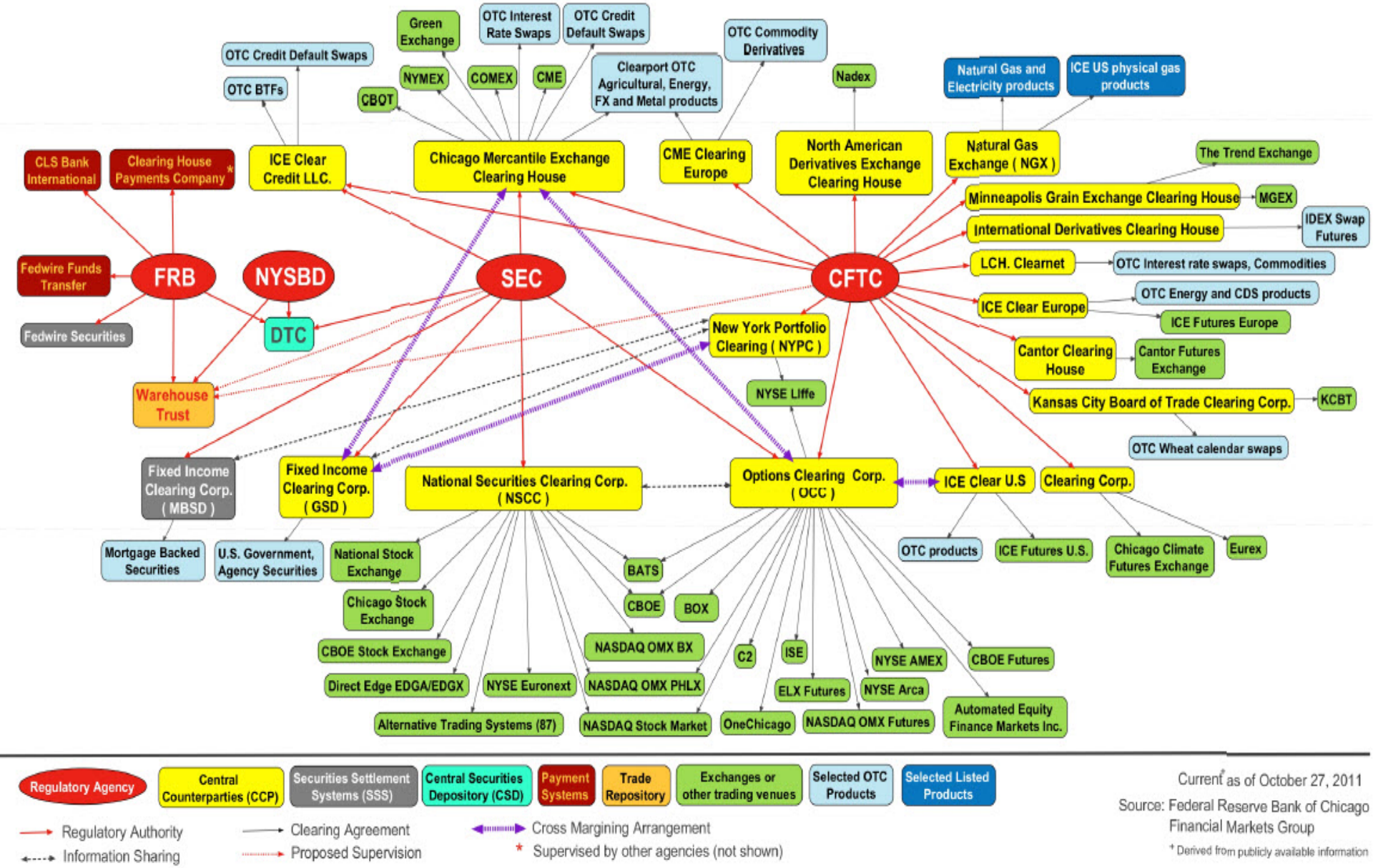


Figure 2: U.S. Regulatory Authority over Payment, Clearing and Settlement Systems



Implications of Complicated Payments

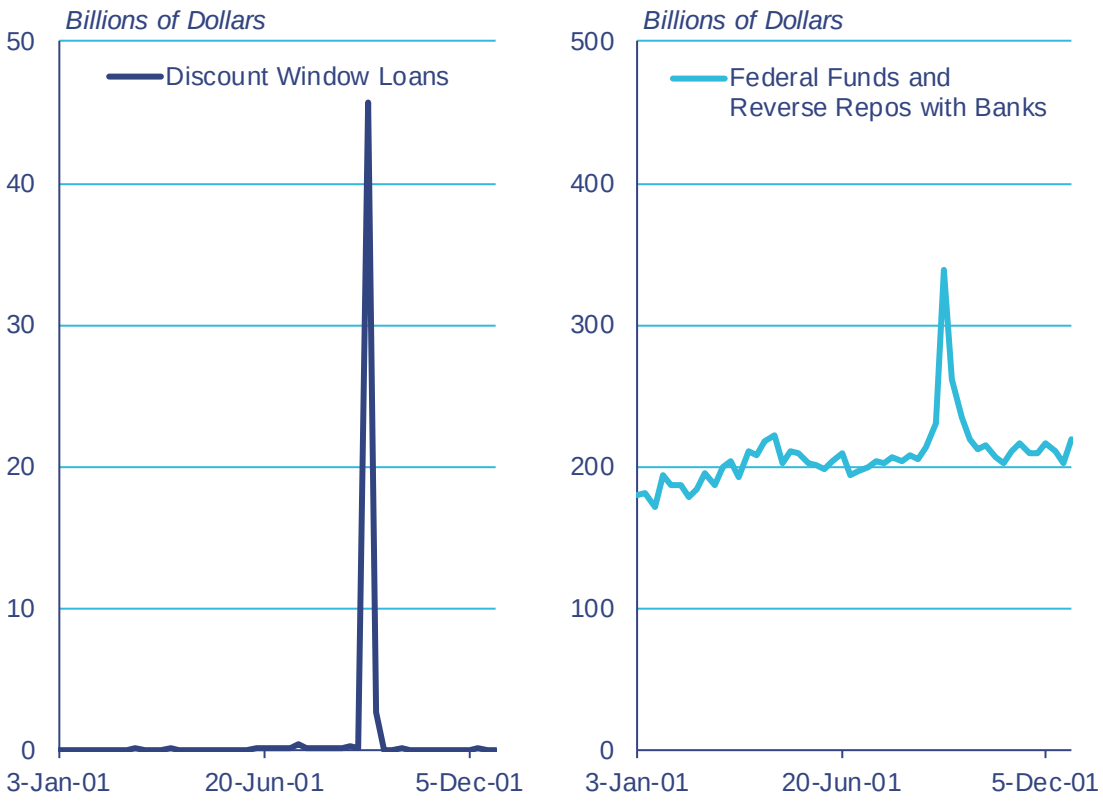
- Advantages
  - Decentralized – difficult to simultaneously shut entire system down
  - Less likely to have a single point of failure
- Disadvantages
  - Cyber attacks focus on weakest link
  - Unified cyber-prevention approach difficult to implement

Disruption of Payments on September 11, 2001

- Numerous payments systems impacted
- New York Stock Exchange halted trading for 4 days
- Flow of funds badly disrupted
- Some banks had a large surplus of reserves and others had large deficits

Figure 3: Federal Reserve Loans to Depository Institutions and Commercial Bank Interbank Loans

Weekly, January 3, 2001 - December 26, 2001



Note: Data are weekly as of Wednesdays.

Source: Federal Reserve Board, Haver Analytics

Remediation after September 11

- Within one week most services had been restored
- *Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*
  - Required expensive back-up capabilities and quick restoration of service
  - Dramatically improved the ability and speed at which payments activities could be restored should a man-made or natural disaster impact operations
- These actions were taken after the problem was apparent

Figure 4: Major Cyber Intrusions Originating from Vendors

Comprised Companies	Quantity of Records Compromised	Description
Target	40 mil. credit cards, 70 mil. customer records	Stolen HVAC vendor login ID and password
Home Depot	56 mil. credit cards, 53 mil. email addresses	Stolen HVAC vendor login ID and password
National Archives & Records Administration	76 mil. veteran records	Computer disk drive sent to 3rd party for destruction
Goodwill Stores	900 thous. credit cards	3rd party POS vendor

Source: Federal Reserve Bank of Boston, Various News Reports

Cyber Security and Smaller Financial Institutions

- Over 6,000 banks in the U.S., many of them small
- Small banks have limited resources for cyber security
  - No access to national security briefings
  - Often rely on outside vendors or third-party processors
- The least technically advanced entities may provide the easiest access for hackers to the payments system

Federal Reserve Bank of Boston and Cyber Security for Small Banks

- Single-industry focused pilot program
  - Information sharing the key component
  - In-person meetings – everyone signs non-disclosure forms
  - Conducted by cyber-security experts within the Boston Fed who have broader access to details about emerging threats and mitigants that may be available to smaller financial institutions
  - Not part of the supervisory process
- We are expanding the program in 2015

Federal Reserve Payment System Study*

- *Strategies for Improving the U.S. Payment System,* paper issued earlier this week
- The Federal Reserve believes that security is the foundation of any payment system
- The Fed intends to promote end-to-end payments security, and encourage a system that improves continuously in response to evolving threats

* *www.FedPaymentsImprovement.org*

Concluding Observations

- Cyber security is a financial stability concern – and the changing nature of threat (less financial gain and more akin to cyber terrorism) poses new challenges
- Central banks need to be proactive
  - Adapt payments system to new threats
  - Consider small as well as large banks
- This is a problem with no boundaries – applies whether you are at the tip of Cape Town or the top of Maine